AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1.   (Previously Presented) A communication system in which an image processing apparatus and a client communicate data with each other through a network,

wherein said image processing apparatus comprises:

a root certificate creator which creates a root certificate including a public key paired with a private key and being signed with the private key;

a second certificate creator which creates, when a connection for communication is requested by said client, a second certificate designating the root certificate created by said root certificate creator as a certificate authority at a higher level and being signed with the private key used to sign the root certificate; and

a communication device which transmits the second certificate created by said second certificate creator to said client; and

wherein said client comprises:

a storage device which has stored therein, before the connection for communication is requested to said image processing apparatus, the root certificate created by said root certificate creator; and

a verifier which verifies the signature of the second certificate received from said image processing apparatus with the root certificate stored in said storage device.

2.   (Previously Presented) The communication system according to claim 1, wherein said image processing apparatus is a printer.

3.   (Previously Presented) The communication system according to claim 1, wherein said image processing apparatus is a multifunctional peripheral.

4.   (Original) The communication system according to claim 1, wherein said client is a personal computer.

5.   (Previously Presented) The communication system according to claim 1, wherein said storage device is a hard disk drive.

6.   (Original) The communication system according to claim 1, wherein said second storage device is a read-only memory.

7.   (Previously Presented) A communication method for a communication system in which an image processing apparatus and a client communicate data with each other through a network,

wherein the image processing apparatus creates a root certificate including a public key paired with a private key and being signed with the private key;

the client installs the root certificate which is created by the image processing apparatus and which includes the public key, prior to the client requesting a connection for communication to the image processing apparatus;

the image processing apparatus creates, when a connection for communication is requested by the client, a second certificate designating the root certificate created by the image processing apparatus as a certificate authority at a higher level and being signed with the private key used to sign the root certificate when data is sent to the client;

the image processing apparatus sends the second certificate to the client; and

the client verifies the signature of the second certificate received from the image processing apparatus with the installed root certificate.

8.   (Previously Presented) The method according to claim 7, wherein the image processing apparatus further holds at least one intermediate certificate for one or more certificate authorities existing in a hierarchical order up to a root certificate authority;

the client installs the at least one intermediate certificate in addition to the root certificate;

the image processing apparatus sends the second certificate to the client; and

the client verifies the signature of the second certificate received from the image processing apparatus with the at least one intermediate certificate installed therein, and verifies the signature of the at least one intermediate certificate received from the image processing apparatus with the root certificate installed therein.

9.   (Previously Presented) The method according to claim 7, wherein when the client installs the root certificate, the client requests the root certificate from the image processing apparatus when a printer driver from the image processing apparatus is installed in the client, receives the root certificate from the image processing apparatus, converts the received root certificate to a predetermined format when the root certificate is received, and installs the converted root certificate.

10.   (Previously Presented) The method according to claim 7, wherein when the client installs the root certificate, the installation is performed after the root certificate is confirmed by a user.

11.   (Previously Presented) The method according to claim 7, wherein the image processing apparatus is a printer, and the client installs the root certificate after a printer driver from the image processing apparatus is installed in the client.

12.   (Previously Presented) The method according to claim 7, wherein the data is communicated according to the security sockets layer (SSL) protocol.

13-16. (Cancelled)

17.   (Previously Presented) An image processing apparatus to be used in a communication system in which the image processing apparatus and a client communicate with each other through a network, the image processing apparatus

sends information to the client, and the client uses the information to communicate

with the image processing apparatus, the image processing apparatus comprising:

a root certificate creator which creates a root certificate including a public key

paired with a private key and being signed with the private key;

a storage device which stores the root certificate signed with the private key;

a second certificate creator which creates, when a connection for

communication is requested by the client, a second certificate designating the root

certificate created by said root certificate creator as a certificate authority at a higher

level and being signed with the private key used to sign the root certificate; and

an interface which sends the information as well as the root certificate

including the public key to the client through the network before the connection for

communication is requested to the image processing apparatus, and sends, after the

root certificate created by said root certificate creator is installed in the client, the

second certificate to the client for verification of the information sent from the image

processing apparatus.

18.   (Previously Presented) The image processing apparatus according to

claim 17, wherein the image processing apparatus is a printer.

19.   (Previously Presented) The image processing apparatus according to

claim 17, wherein the information is a printer driver.

20.   (Previously Presented) The communication system according to claim

1, wherein the root certificate is stored in said storage device of said client prior to

the transmission of the second certificate to said client from said communication device.

21.   (Cancelled)

22.   (Previously Presented) The communication system according to claim 1, wherein said verifier is operable to verify the signature of the second certificate by decrypting the public key of the root certificate stored in said storage device to obtain a first hash value, calculating a second hash value of the second certificate received from said image processing apparatus, and comparing the first and second hash values to determine if they are equal to each other.

23.   (Previously Presented) The method according to claim 7, wherein the image processing apparatus sends the second certificate to the client after the root certificate is installed in the client.

24.   (Previously Presented) The method according to claim 8, wherein the client installs the at least one intermediate certificate prior to receiving the second certificate from the image processing apparatus.

25-27. (Cancelled)

28.   (Previously Presented) The communication system according to claim 1, wherein:

the storage device of said client has stored therein, before the connection for
communication is requested to said image processing apparatus, the public key of
the root certificate; and

the verifier verifies the signature of the second certificate received from said
image processing apparatus by decrypting the second certificate with the public key
of the root certificate stored in said storage device of said client.

29.   (Previously Presented) The communication method according to claim
7, wherein:

the client stores the public key of the installed root certificate, prior to the
client requesting the connection for communication to the image processing
apparatus; and

the client verifies the signature of the second certificate received from the
device by decrypting the second certificate with the public key of the root certificate
stored in the client.

30.   (Cancelled)

31.   (Previously Presented) A computer-readable recording medium having
a computer program recorded thereon for causing a computing device, which is
communicatively coupled to the computer-readable recording medium and which is
configured to communicate with a client through a network to send information to the
client, which uses the information to communicate with the computing device, to
perform operations comprising:

storing a pair of a public key and a private key;

creating a root certificate including the public key and private key and being

signed with the private key;

storing the root certificate signed with the private key;

sending the information and the root certificate created by the computing

device and including the public key to the client, before a request for communication

is requested by the client;

creating, when the connection for communication is requested by the client, a

second certificate designating the root certificate created by the computing device as

a certificate authority at a higher level and being signed with the private key used to

sign the root certificate; and

sending, after the root certificate has been installed in the client, the created

second certificate to the client for verification of the information sent from the

computing device.

32.   (Previously Presented) The computer-readable recording medium

according to claim 31, wherein the computing device is printer.

33.   (Previously Presented) The computer-readable recording medium

according to claim 31, wherein the information is a printer driver.

34.   (New) The communication system according to claim 1, wherein the

connection for communication requested by said client is a request for encrypted

communication between said image processing apparatus and said client after the root certificate created by said image forming apparatus is installed in said client.

35.   (New) The communication method according to claim 7, wherein the connection for communication requested by said client is a request for encrypted communication between said image processing apparatus and said client after the root certificate created by said image forming apparatus is installed in said client.

36.   (New) The image processing device according to claim 17, wherein the connection for communication requested by said client is a request for encrypted communication between said image processing apparatus and said client after the root certificate created by said image forming apparatus is installed in said client.

37.   (New) The computer-readable recording medium according to claim 31, wherein the connection for communication requested by said client is a request for encrypted communication between said computing device and said client after the root certificate created by said computing device is installed in said client.

38.   (New) An image forming apparatus which communicates with a client through a network, the image forming apparatus comprising:

a storage device which stores a first certificate created in the image forming apparatus; and

a communication device which transmits the first certificate stored by the storage device to the client for installation;

wherein the communication device is configured to transmit a second

certificate, which includes path information to the first certificate stored in the image

forming apparatus, to the client when a connection for encrypted communication is

requested by the client after the first certificate stored in the image forming apparatus

is installed in the client.

39.   (New) The image forming apparatus according to claim 38, wherein the

image forming apparatus includes a scanner and a printer.

40.   (New) The image forming apparatus according to claim 38, wherein the

image forming apparatus is a multi-functional peripheral.

41.   (New) The image forming apparatus according to claim 38, wherein the

storage device is a hard disk drive.

42.   (New) The image forming apparatus according to claim 38, wherein

the second certificate transmitted to the client after the first certificate stored in the

image forming apparatus is installed in the client, is in the same format as the first

certificate stored in the image forming apparatus.

43.   (New) The image forming apparatus according to claim 38, wherein

the second certificate includes an identification of an issuer of the first certificate

stored in the image forming apparatus

44.   (New) An image forming apparatus which communicates with a client

through a network, the image forming apparatus comprising:

a storage device which stores a first certificate created in the image forming

apparatus; and

a communication device which transmits the first certificate stored by the

storage device to the client based on a designation by the client;

wherein the communication device is configured to transmit a second

certificate which includes path information to the first certificate stored in the image

forming apparatus, to the client when a connection for encrypted communication is

requested by the client in which the first certificate stored in the image forming

apparatus is installed.

45.   (New) The image forming apparatus according to claim 44, wherein the

image forming apparatus includes a scanner and a printer.

46.   (New) The image forming apparatus according to claim 44, wherein the

image forming apparatus is a multi-functional peripheral.

47.   (New) The image forming apparatus according to claim 44, wherein the

storage device is a hard disk drive.

48.   (New) The image forming apparatus according to claim 44, wherein the

second certificate transmitted to the client after the first certificate stored in the image

forming apparatus is installed in the client, is in the same format as the certificate

stored in the image forming apparatus.

49.   (New) The image forming apparatus according to claim 44, wherein

the second certificate includes an identification of an issuer of the first certificate

stored in the image forming apparatus.